

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum


*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Sylvain Guilley (Ed.)

# Constructive Side-Channel Analysis and Secure Design

8th International Workshop, COSADE 2017  
Paris, France, April 13–14, 2017  
Revised Selected Papers

*Editor*  
Sylvain Guilley   
Secure-IC S.A.S. and TELECOM-ParisTech  
Paris  
France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-64646-6              ISBN 978-3-319-64647-3 (eBook)  
DOI 10.1007/978-3-319-64647-3

Library of Congress Control Number: 2017947503

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The 8th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017) was organized by and held at Télécom ParisTech, Paris, France, during April 13–14, 2017. The host was the Paris 13th district site of Télécom ParisTech, which is also known as the LTCI (*Laboratoire Traitement et Communication de l'Information*) of Université Paris-Saclay. The workshop was financially sponsored by five golden sponsors, namely, AlphaNov, ANSSI, NewAE Technology, Riscure, and Secure-IC S.A.S. The company INVIA was a silver sponsor of the event.

The excellent arrangements were led by the COSADE 2017 general chair, Prof. Jean-Luc Danger, and organizing chair, Prof. Guillaume Duc. They were helped by a highly motivated team of PhD students from our SEN (*Systèmes Électronique Numérique*) research group, namely, Nicolas Bruneau, Sébastien Carré, Éloi de Chérissey, Margaux Dugardin, Khaled Karray, Damien Marion, Martin Moreau, Alexander Schaub, and Michaël Timbert. This year COSADE provided an open forum for exchanging and sharing of ongoing hot issues and results of research, development, and applications in the analysis of attacks and design of protection against attacks on embedded devices.

The Program Committee prepared for an interesting program, including two invited talks, namely, from Dr. Victor Lomné (ANSSI), talking on “Overview of Fault-based Cryptanalysis on Block Ciphers,” and Prof. Philippe Maurine (LIRMM), about the question “Impacts of Technology Trends on Physical Attacks?”. The technical program also included an industrial exhibition show, which allowed for fruitful discussions about applications of basic research for transfer to industry.

The workshop had seven sessions built from the contributed papers: on Thursday, “Side-Channel Attacks and Technological Effects,” “Side-Channel Countermeasures,” “Algorithmic Aspects in Side-Channel Attacks,” and on Friday, “Side-Channel Attacks,” “Fault Attacks,” “Embedded Security,” and “Side-Channel Tools.”

We would like to thank all authors who submitted papers. Each paper was reviewed by at least three reviewers. The 25 external reviewers as well as the 26 Program Committee members contributed to the reviewing process from their particular areas of expertise. The reviewing and active discussions were facilitated by the EasyChair Web-based system. Through the system, we could check the amount of similarity between the submitted papers and previously published papers to prevent plagiarism and self-plagiarism. Following the strict reviewing processes, 16 outstanding papers from eight countries (Austria, Belgium, France, Germany, Japan, Korea, The Netherlands, and Switzerland) were accepted for publication in this volume of *Lectures Notes in Computer Science* by Springer (LNCS Vol. 10348). I would also like to thank the session chairs (Naofumi Homma, François-Xavier Standaert, Jens-Peter Kaps, Benoît Feix, Benoît Gérard, Yannick Téglia, Pierre-Yvan Liardet, Jean-Luc Danger, and Guillaume Barbu) for their commitment to COSADE.

The workshop featured a welcome reception on the evening of Wednesday April 12, and a social event on board the *Bateaux Mouches* (cruising dinner on the Seine) on Thursday, April 13. During this enjoyable event, François-Xavier Standaert was awarded for the nearest distance with respect to COSADE, and Werner Schindler received the random lottery special prize.

Many people contributed to the success of COSADE 2017. We would like to express our deepest appreciation to each of the COSADE Organizing and Program Committee members as well as the paper contributors. Without their endless support and sincere dedication and professionalism, COSADE 2017 would have been impossible.

May 2017

Sylvain Guilley

# Organization

## Program Committee

Shivam Bhasin	Temasek Labs@NTU, Singapore
Christophe Clavier	Université de Limoges, France
Hermann Drexler	Giesecke & Devrient, Germany
Cécile Dumas	CEA, France
Thomas Eisenbarth	WPI, USA
Wieland Fischer	Infineon, Germany
Christophe Giraud	Oberthur Technologies, France
Johann Groszschäedl	University of Luxembourg, Luxembourg
Sylvain Guilley	GET/ENST, CNRS/LTCI, France
Benoît Gérard	DGA-MI, France
Tim Güneysu	University of Bremen and DFKI, Germany
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohoku University, Japan
Michael Hutter	Cryptography Research, USA
Thanh Ha Le	SAFRAN, France
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Houssem Maghrebi	SAFRAN Identity and Security, France
Marcel Medwed	NXP Semiconductors, Austria
Amir Moradi	Ruhr University Bochum, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Stjepan Picek	KU Leuven, Belgium
Francesco Regazzoni	ALaRI – USI, Switzerland
Matthieu Rivain	CryptoExperts, France
Kazuo Sakiyama	The University of Electro-Communications, Tokyo, Japan
Ruggero Susella	STMicroelectronics, Italy
Carolyn Whinnall	University of Bristol, UK

## Additional Reviewers

Alessio, Davide	Chabrier, Thomas
Bauer, Sven	Chattopadhyay, Anupam
Bhasin, Shivam	Chen, Cong
Bocktaels, Yves	Dabosville, Guillaume
Breier, Jakub	De Mulder, Elke
Burri, Samuel	Debande, Nicolas
Cagli, Eleonora	Dinu, Daniel

Grosso, Vincent  
Hoffmann, Lars  
Jungk, Bernhard  
Kavun, Elif Bilge  
Le Corre, Yann  
Murray, Bruce  
Nikov, Ventzi  
Patranabis, Sikhar  
Pilato, Christian  
Prouff, Emmanuel  
Reynaud, Léo  
Richter, Bastian  
Rondepierre, Franck

Saha, Sayandeep  
Schneider, Tobias  
Seker, Okan  
Stöttinger, Marc  
Szerwinski, Robert  
Tunstall, Michael  
Ueno, Rei  
Vadnala, Praveen Kumar  
Valencia, Felipe  
Wenger, Erich  
Yamamoto, Dai  
Yli-Mäyry, Ville



# Contents

Does Coupling Affect the Security of Masked Implementations? . . . . .	1
<i>Thomas De Cnudde, Begül Bilgin, Benedikt Gierlichs, Ventsislav Nikov, Svetla Nikova, and Vincent Rijmen</i>	
Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study . . . . .	19
<i>Kashif Nawaz, Dinal Kamel, François-Xavier Standaert, and Denis Flandre</i>	
Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks: A Practical Security Evaluation on FPGA . . . . .	34
<i>Florian Unterstein, Johann Heyszl, Fabrizio De Santis, and Robert Specht</i>	
Toward More Efficient DPA-Resistant AES Hardware Architecture Based on Threshold Implementation . . . . .	50
<i>Rei Ueno, Naofumi Homma, and Takafumi Aoki</i>	
Enhanced Elliptic Curve Scalar Multiplication Secure Against Side Channel Attacks and Safe Errors . . . . .	65
<i>Jeremy Dubeuf, David Hely, and Vincent Beroulle</i>	
SafeDRP: Yet Another Way Toward Power-Equalized Designs in FPGA . . . .	83
<i>Maik Ender, Alexander Wild, and Amir Moradi</i>	
On the Construction of Side-Channel Attack Resilient S-boxes . . . . .	102
<i>Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch</i>	
Efficient Conversion Method from Arithmetic to Boolean Masking in Constrained Devices . . . . .	120
<i>Yoo-Seung Won and Dong-Guk Han</i>	
Side-Channel Analysis of Keymill . . . . .	138
<i>Christoph Dobraunig, Maria Eichlseder, Thomas Korak, and Florian Mendel</i>	
On the Easiness of Turning Higher-Order Leakages into First-Order . . . . .	153
<i>Thorben Moos and Amir Moradi</i>	

Side-Channel Attacks Against the Human Brain: The PIN Code Case Study . . . . .	171
<i>Joseph Lange, Clément Massart, André Mouraux, and Francois-Xavier Standaert</i>	
Impacts of Technology Trends on Physical Attacks? . . . . .	190
<i>Philippe Maurine and Sylvain Guilley</i>	
Low-Cost Setup for Localized Semi-invasive Optical Fault Injection Attacks: How Low Can We Go?. . . . .	207
<i>Oscar M. Guillen, Michael Gruber, and Fabrizio De Santis</i>	
DFA on LS-Designs with a Practical Implementation on SCREAM. . . . .	223
<i>Benjamin Lac, Anne Canteaut, Jacques Fournier, and Renaud Sirdey</i>	
Multiple-Valued Debiasing for Physically Unclonable Functions and Its Application to Fuzzy Extractors . . . . .	248
<i>Manami Suzuki, Rei Ueno, Naofumi Homma, and Takafumi Aoki</i>	
Getting the Most Out of Leakage Detection: Statistical Tools and Measurement Setups Hand in Hand. . . . .	264
<i>Santos Merino del Pozo and François-Xavier Standaert</i>	
Mind the Gap: Towards Secure 1st-Order Masking in Software . . . . .	282
<i>Kostas Papagiannopoulos and Nikita Veshchikov</i>	
<b>Author Index</b> . . . . .	299